International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 113-118

TRANS STELLAR
Journal Publications • Research Consultancy

A REVIEW OF ONE TIME PASSWORD MOBILE VERIFICATION

SHALLY[1] & GAGANGEET SINGH AUJLA[2]

[1]Research Fellow, Chandigarh Engineering College, Mohali, Punjab, India

[2]Assistant Professor, Chandigarh Engineering College, Mohali, Punjab, India

ABSTRACT

Use of mobile phone is quite common in the modern day environment .With the increase in the facilities for the users of different sectors, data theft has also increased. To prevent the authentication process from the data theft, one time password system is applied to various sector of the industry like if you are logging in into an account, you need a OTPK password to get verified that you are the authenticated user. In such a case the user must be registered to the network to get the OTPK password. This paper focuses on the different aspects of OTPK and the ways of creation of this system.

KEYWORDS: OTPK, Mobile Users, Authentication

INTRODUCTION

One time password (OTP) is a password that is only valid for a single login session or transaction. OTP is widely used as a password that is not planted in the database, but only as a single use password and immediately forfeited. The benefit of the OTP is located on the different application with a static password which is planted in the database. The use of encrypted static passwords are also not immune from the attack by using a key logger or sort of it, because if an attacker managed to get the main password and OTP password still login and transactions will not be processed because the password is no longer valid. Code generation as encryption is using Message-Digest Algorithm 5 (MD5) which are widely used with 128-bit hash value, this algorithm has been widely used for security applications, password encryption, and integrity test of a file. [1]

The application of Dynamic Mobile Token uses three codes consisting of epoch time as the key of one time password, the value of the "secret" variable in which each utilizer has a different value so that when it degenerate concurrently, it will result in different value, and 4 digit desultory value between 1000 and 9999 resulting from the website. These three values are then amalgamated and encrypted with md5 algorithm to engender the output of the value of 128 bits or 32 hexadecimal numbers. Only first 6 digits of the hexadecimal number are utilized from the result of the output.

The level security of the password is good enough to double the security in an account and the login process, because each password OTP is only valid once and if you do any mistake, the code generated from the website will change anyway. The time period of the password's life span is 180 seconds, the time to break the OTP password in ratio is 166 = 16,777,216 possibilities in a single input of passwords.

MOBILE TOKEN CONCEPT

Dynamic Mobile Token has a concept to secure online transactions. Mobile Token becomes an additional factor in the authentication process, to prove that the user who do the login session or transaction process is a legitimate user.

Authentication Method

The aim of authentication is to prove that the accessing utilizer is the authentic utilizer. There are many methods that can prove it, but for authentication methods can be optically discerned in the three categories of methods:

- Something You Know It is the most mundane authentication method. This method is relying on the confidentiality of information, such as PIN. This method surmises that no one kens the secret unless the utilizer itself.
- Something You Have This is customarily an adscititious factor to engender a more secure authentication. This method relies on items which conventionally are unique, for examples, the magnetic card/smartcard, hardware tokens, USB tokens, and else. This method postulates that no one has the hardware unless the utilizer itself.
- Something You Are This is the most infrequently utilized method because of technology and the human factor as well. This method relies on the uniqueness of the body components that is not subsist in others such as fingerprint, voice, retina or fingerprint. This method postulates that the components of the body such as fingerprints and retina are different with others.

Password Mode

Dynamic Mobile Token there are two mode used:

- **Challenge/Response Mode (C/R):** This mode is most often used when doing transaction. In this mode the server provides a challenge in the form of a series of numbers. That number must be entered into the Mobile Token to get an answer (replication). Then the utilizer enters the number that appears on its own Mobile Token into text box on the website. Mobile Token will issue a different code though with the same code challenge. Periodically depending on the time when we answer the challenge in a token.
- **Self Generated Mode (Response Only):** In this mode the server does not give any kind of value (challenge). Mobile Token users can directly issue a series of amalgamation of numbers and letters without having to enter the challenge. As the mode C/R, Mobile Token withal issued different codes periodically depending on the time when the token is authoritatively mandated to engender self-engendered code.[2]

SECURITY LEVEL

At the actual level of security in C/R and Self Generated (Response Only) mode is nothing but the password as well. However, it is different from the password used to login, passwords from Mobile Token has limitation for security reasons, namely:

- **May Only be Used One Time:** Once a password is used, the same password can no longer be used for the second time. With this way, there is no point to intercept the degenerated passwords of Mobile Token because the password cannot be used again. However, if the password is managed to be intercepted so it never gets to the server, it is still a valuable password as the server password has not been used.

- **May Only be Used within a Limited Time Span:** Mobile Token generated passwords have a very limited life, probably between 2-3 minutes. When the age expires, the password cannot be used anymore, although it has never been used. Time is a very critical element in this system of Mobile Token
- **May Only be Used in the Narrow Context:** If the password / PIN used for - login is a free context password, in the sense that with the password only, it can do many things, from seeing balances, check transaction and else. But the token generated password can only be used in a narrow context, for example, the password that is used to buy a credit to the number 08123456789, is cannot be used to transfer funds.

GENERAL DESIGN SYSTEM

Authentication Process

Such as passwords in general, on condition that authentication prosperous is the password that is sent to the client is identically tantamount passwords stored on the server. With security reasons infrequently server stores utilizer passwords in plaintext form. Commonly, server stores utilizer passwords in hash form so it cannot be returned in plaintext form. So prosperous authentication requisites can be interpreted as the result of the calculation hash of the password sent by the client must be identically tantamount with the hash value stored in the server (see Figure 1). [3]

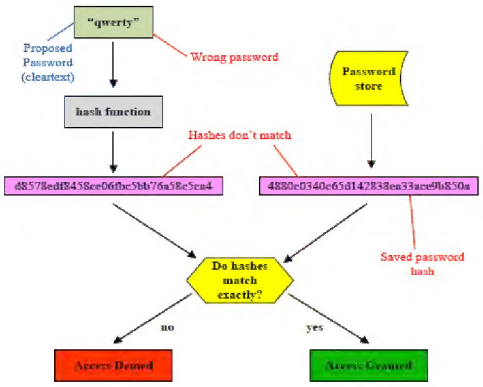

Figure 1: Hash Password Authentication Process

Mobile Token process of authentication on the server has a very critical time distinction. Users have to match the clock in the phone with the clock on the server, the difference in hours that sanctioned is less than 3 minutes and more than 3 minutes, more than that is considered erroneous or the code has been utilized. The chain process of the connection system between the server, client, utilizer, Mobile Token, and the website has a vigorous connection and cannot be dissevered. If one system crash, the other series cannot be commenced or processed (see Figure 2).

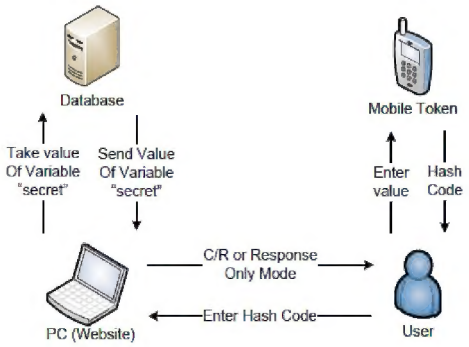

Figure 2: Connection Process in General

One Time Password Process

To avoid brute-forces attacks to the hash value stored in the server, before the user's password is generating its hash value, firstly, add a random string called the salt. In the program, the value of salt is the value of the variable in the Mobile Token secret and also planted in the database. For example, if the user's password is "qwerty", before it generates its hash value, password is added salt in the form value of the secret variable for example "7fc04db" .So the hash value will be calculated three values combined into "qwerty7fc04db" not only "qwerty".

When viewed from the MD5 value "qwerty7fc04db" is "77ed461ee664d2bb7ab75c16f338e943", while the value of MD5 original password without the combination "qwerty" is "d8578edf8458ce06fbc5bb76a58c5ca4". If the passwords do not use salt, then the attacker can easily decrypt the password using a brute force attack or rainbow table to get the value of the password in plain-text, since the site to store database decrypted already widely available. And it is impossible for attacker to build a database for mapping between the plaintext and hash completely.

One-Time Passwords via SMS

One-Time Passwords are utilized as a supplemental factor in multi-factor sanction/authentication applications. They are only valid for precisely one sanction or authentication request. To evade password lists, a convenient way to provide the utilizer with an OTP is to send it through SMS. The phone number of the utilizer must be registered for the accommodation that provides SMS OTPs for authentication or sanction. OTPs are quite popular as a supplemental sanction or authentication factor in web-predicated accommodations. These passwords can be utilized to authenticate a utilizer, I. e., the utilizer needs a valid OTP to prove his identity to authenticate in to a web application or to access the company's private network. SMS OTPs are withal utilized for account verification, e. g., Google Mail. Recently, the online storage accommodation Drop box integrated SMS-predicated two factor authentication after facing some security issues. Online games such as Blizzard's Battle.net have withal commenced utilizing SMS for account unlocking. Another application for OTPs is sanction. Here, the OTP is bound to a certain request or transaction in order to attest it. Additionally, the One Time Password can be restricted to a very short time window. In online banking web applications for example, the utilizer has to authenticate him through a valid username and password to start a transaction. Directly after this transaction request, the utilizer gets a message containing the OTP that must be supplementally entered to sanction the transaction. In this application area the OTP is called a mobile Transaction Authorization Number (mobile TAN or man).[4]

SMS OTP THREAT MODEL

The attacker's goal is the acquisition of the OTP, and for this he has several options such as wireless interception or mobile phone Trojans. Less known attacks such as the SIM Swap Attack can also be used. Below we further discuss the widely used attacks. Note that as the attacks target SMS interception in general, they can be used against all SMS OTP systems.

MOBILE PHONE TROJANS

Mobile phone malware especially Trojans which are designed to intercept SMS messages containing OTPs, are a elevating threat. This kind of malware is engendered by malefactors directly for the purpose of making money. In the following, we provide an overview of the different kinds of SMS OTP purloining Trojans. The ZITMO

(Zeus in the Mobile) Trojan for Simian OS is the first known piece of malware that was specifically created for intercepting means.

The ZITMO binary is distributed as a mundane signed Simian application. It possesses the required capabilities in order to register itself with the Simian Operating System to receive messages when they arrive from the mobile network. Upon reception it can forward SMS to a predefined mobile number. Besides the capability to forward SMS, ZITMO can additionally expunge messages. This capability can be acclimated to thoroughly obnubilate the fact that an SMS message SMS-Based One-Time Passwords: Attacks and Defence 153 containing man ever arrived at the infected phone. Further, the ZITMO Trojan can be remotely reconfigured via SMS. Through this the assailant can, for example, transmute the destination number for forwarded SMS. In February 2011, a Zeus version for Windows Mobile was detected and designated Trojan-Spy.WinCE.Zbot.a. The Trojan contained the same rudimental functionality as ZITMO. Similar Trojans additionally subsist for Android and RIM's Black Berry. Additionally, further mobile malware, which purloins authentication credentials, attacks mobile phone owners. All known SMS OTP Trojans are utilizer-installed malware. This denotes they do not leverage any security susceptibility of the affected platform. Instead, they utilize convivial engineering to illude the utilizer into installing the binary.

CONCLUSIONS

With all the made survey over here, it is concluded that the One time password is a very important part in every sector of the industry. This paper concludes about the methods of creation of the one time password generation system and effect of Trojans in the system.

REFERENCES

1. Sagar Acharya, "Two Factor Authentication Using Smartphone Generated One Time Password ", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 85-90 www.iosrjournals.org.
2. Collin Mulliner, "SMS-Based One-Time Passwords: Attacks and Defense", Northeastern University crm@ccs.neu.edu.
3. Dinei Florence, "One-Time Password Access to Any Server without Changing the Server", Microsoft Research, One Microsoft Way, Redmond, WA dinei@microsoft.com, c.herley@ieee.org.
4. M. Viju Prakash, "Eliminating Vulnerable Attacks Using One-Time Password and Pass Text – Analytical Study of Blended Schema", Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, Nov. 2010. © 2010 UniCSE, ISSN: 2219-2158